UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

IN RE: CLEVELAND BROTHERS DATA INCIDENT LITIGATION	**Case No. Case 1:23-cv-00501-JPW**
	CLASS ACTION
	CONSOLIDATED COMPLAINT

Representative Plaintiffs allege as follows:

INTRODUCTION

1. Representative Plaintiffs Randy Thomas, Gabrielle Thomas, and Robert MacMichael ("Representative Plaintiffs") bring this class action against Defendant Cleveland Brothers Equipment Company, Inc. ("Defendant" or "Cleveland Brothers") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' personally identifiable information stored within Defendant's information network, including without limitation full names and Social Security numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as "personally identifiable information" or "PII").[1]

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and at least 8,600[2] other similarly situated persons in this preventable cyberattack purportedly discovered by Defendant on

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[2] *Breach Portal*, https://apps.web.maine.gov/online/aeviewer/ME/40/dc9e2660-126f-4259-b1dd-44be29241f38.shtml (last accessed February 27, 2023).

November 3, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII, which was being kept unprotected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that the PII was maintained in a manner consistent with industry and other relevant standards.

4. While Defendant claims to have discovered the breach as early as November 3, 2022, Defendant did not begin informing victims of the Data Breach until February 17, 2023 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it. The notice received by Representative Plaintiffs was dated February 17, 2023.

5. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PII.

6. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations as well as common law principles.

7. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding

the encryption of data, even for internal use. As a result, the PII of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class, and at least one other Class Member is a citizen of a state different from Defendant.

9. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

10. Defendant is headquartered in and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and/or services within this State.

11. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District, and Defendant is located in this Judicial District.

PLAINTIFFS

12. Representative Plaintiff Randy Thomas is a resident and citizen of Florida, currently residing in Fort Myers, Florida. Mr. Thomas received the Notice Letter, via U.S. mail, directly from Defendant, dated February 17, 2023. As a former employee of Defendant, Mr. Thomas provided his PII to Defendant as a necessary condition of his employment with Defendant and on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his PII. If Mr. Thomas had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

13. Representative Plaintiff Gabrielle Thomas is a resident and citizen of Florida, currently residing in Fort Myers, Florida. Ms. Thomas received the Notice Letter, via U.S. mail, directly from Defendant, dated February 17, 2023. As the spouse of a former employee of Defendant, Ms. Thomas provided her PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII. If Ms. Thomas had known that Defendant would not adequately protect her PII, she would not have entrusted Defendant with her PII or allowed Defendant to maintain this sensitive PII.

14. Representative Plaintiff Robert MacMichael is a resident and citizen of Pennsylvania. Mr. MacMichael received the Notice Letter, via U.S. mail, directly from Defendant, dated February 17, 2023. As a former employee of Defendant, Mr. MacMichael provided his PII to Defendant as a necessary condition of his employment with Defendant and on the condition that it be maintained as confidential and with the reasonable understanding that Defendant would employ reasonable safeguards to protect his PII. If Mr. MacMichael had known

that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

15. Defendant received highly sensitive personal information from Representative Plaintiffs. As a result, Representative Plaintiffs' information was among the data accessed by an unauthorized third party in the Data Breach.

16. Representative Plaintiffs' PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiffs' PII. This PII was within the possession and control of Defendant at the time of the Data Breach.

17. Representative Plaintiffs received a letter from Defendant, dated February 17, 2023, stating that their PII was involved in the Data Breach (the "Notice").

18. As a result, Representative Plaintiffs spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring accounts, and seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

19. Representative Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

20. Representative Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling their PII.

21. Representative Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

22. Representative Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

23. Defendant Cleveland Brothers is a Delaware corporation with a principal place of business located at 4565 William Penn Highway, Murrysville, Pennsylvania 15668.

24. According to Defendant's LinkedIn, Defendant is a construction equipment dealership with over 25 locations, through which Defendant supplies "construction equipment, parts and service, industrial diesel and gas engines and generators, oil and gas machinery [and] on-highway trucks."[3]

25. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

26. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following classes/subclass(es) (collectively, the "Class"):

[3] https://www.bloomberg.com/profile/company/0178371D:US (last accessed February 27, 2023).

Nationwide Class:
"All individuals within the United States of America whose PII information was exposed to unauthorized third parties as a result of the data breach discovered on November 3, 2022."

Florida Subclass:
"All individuals within the State of Florida whose PII information was exposed to unauthorized third parties as a result of the data breach discovered on November 3, 2022."

Pennsylvania Subclass:
"All individuals within the State of Pennsylvania whose PII information was exposed to unauthorized third parties as a result of the data breach discovered on November 3, 2022."

27. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

28. Also, in the alternative, Representative Plaintiffs request additional Subclasses as necessary based on the types of PII that were compromised.

29. Representative Plaintiffs reserve the right to amend the above definition or to propose Subclasses in subsequent pleadings and motions for class certification.

30. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that

basis, allege the total number of Class Members is in the thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiffs and Class Members that their PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Representative Plaintiffs and Class Members;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff

Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Classes in their entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

31. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Classes in their entirety, not on facts or law applicable only to Representative Plaintiffs.

32. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

33. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the

Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Background

34. Defendant is a company that boasts itself as being Pennsylvania's largest CAT dealership, selling "new, used and rental equipment of all sizes, engines, generators, air compressors and much more."

35. Representative Plaintiffs and Class Members are current and former employees of Defendant's and/or beneficiaries of employee benefits provided by Defendant.

36. In order to apply to be an employee or obtain certain employment-related benefits at Defendant, Representative Plaintiffs and Class Members were required to provide sensitive and confidential PII, including their names and Social Security numbers.

37. The information held by Defendant in its computer systems included the unencrypted PII of Representative Plaintiffs and Class Members.

38. Upon information and belief, in the course of collecting PII from employees, including Representative Plaintiffs, Defendant promised to provide confidentiality and adequate security for employee data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

39. Indeed, Defendant's Privacy Statement provides that: "[w]e will not sell or rent your information to any third party and will exercise reasonable efforts to keep the information secure. Cleveland Brothers Equipment Co., Inc. recognizes and respects your online privacy."

40. Representative Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

41. Representative Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Representative Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Representative Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

42. Defendant had a duty to adopt reasonable measures to protect the PII of Representative Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its employees' PII safe and confidential.

43. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Representative Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

44. Defendant derived a substantial economic benefit from collecting Representative Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

45. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Representative Plaintiffs' and Class Members' PII from disclosure.

The Cyberattack

46. On or about February 17, 2023, Defendant began sending Plaintiffs and other victims of the Data Breach an untitled notice letter, informing them that:

> **What Happened?** On November 5, 2022, we discovered unusual activity on our network. We immediately began an investigation, which included working with third-party

> specialists to determine the nature and scope of the activity. Our investigation determined an unknown party accessed parts of our network between November 3, 2022 and November 5, 2022. Therefore, we conducted a review of our network to determine the type of information contained therein and to whom the information related.
>
> **What Information Was Involved?** On January 31, 2023, after a thorough review, we determined the type of information included your name and the following: your name and Social Security number.[4]

47. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to full names and Social Security numbers. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

48. According to the Data Breach Notification, which Defendant filed with the Maine Attorney General, 8,600 persons were affected by the Data Breach.[5]

49. Representative Plaintiffs were provided the information detailed above upon their receipt of a Notice Letter from Defendant, dated February 17, 2023. Representative Plaintiffs were not aware of the Data Breach—or even that Defendant was still in possession of their data until receiving that Notice Letter.

50. Omitted from the Notice Letter were the dates of Defendant's investigation of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took over three months to inform impacted individuals after Defendant detected the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Representative Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

---

[4] Notice Letter.

[5] Breach Portal, https://apps.web.maine.gov/online/aeviewer/ME/40/dc9e2660-126f-4259-b1dd-44be29241f38.shtmlf (last accessed February 27, 2023).

51. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Representative Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Representative Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

Defendant's Failed Response to the Breach

52. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Representative Plaintiffs' and Class Members' PII.

53. Not until roughly three months after Defendant claims to have discovered the Data Breach did it begin sending the Notice to persons whose PII Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant' recommended next steps.

54. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on November 3, 2022 and had taken steps to respond.

55. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Representative Plaintiffs' and Class Members' PII.

56. Defendant had and continues to have obligations created by reasonable industry standards, common law, and its own assurances and representations to keep Representative Plaintiffs' and Class Members' PII confidential and to protect such PII from unauthorized access.

57. Representative Plaintiffs and Class Members were required to provide their PII and to Defendant as a condition of employment or a condition of receiving employee benefits. Defendant created, collected, and stored Representative Plaintiffs' and Class Members' data with

the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

58. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

59. Representative Plaintiffs' and Class Members' PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Representative Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the PII of Representative Plaintiffs and Class Members.

Data Breaches Are Preventable.

60. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

61. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

[6] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

[7] *Id.* at 3-4.

62. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[8]

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Oct. 17, 2022).

63. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware

Scan Interface] for Office [Visual Basic for Applications].[9]

64. Given that Defendant were storing the sensitive PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

65. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over 8,000 current and former employees and other personnel, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, And Stores Its Employees' PII

66. As a condition of employment with Defendant or to obtain employment-related benefits, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

67. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to perform its business services.

68. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

69. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained

[9] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

70. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

71. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

72. Indeed, Defendant's Privacy Policy provides that: "Cleveland Brothers Brands will take commercially and technologically reasonable precautions to protect your information while it is in our possession."[10]

Defendant Knew, Or Should Have Known, Of the Risk Because Employers In Possession Of PII Are Susceptible To Cyber Attacks

73. Data thieves regularly target companies like Defendant due to the highly sensitive information that they hold in custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

74. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

75. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

[10] https://www.Cleveland Brothersbrands.com/privacy-statement

records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

76. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

77. Additionally, as companies became more dependent on computer systems to run their business,[12] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[13]

78. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

79. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[14]

---

[11] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

[12] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[13] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

[14] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

80. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[15]

81. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

82. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

83. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

84. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

[15] *Id.*

85. Defendant's offering of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

86. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

87. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

88. As an employer in possession of its current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Had an Obligation to Protect the Stolen Information

89. Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' sensitive data breaches duties it owes Representative Plaintiffs and Class Members under statutory and common law. Representative Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

90. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

91. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Representative Plaintiffs and Class Members.

92. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

93. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

94. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

95. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

96. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

97. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

98. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

99. PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites.

100. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details

have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[18]

101. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

102. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

103. Identity thieves can use PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as

---

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

104. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

105. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

106. When cybercriminals access personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

107. And data breaches are preventable.[20] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).
[20] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

security solutions."[21] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[22]

108. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[23]

109. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

110. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PII and/or financial information; (iii) failing to take standard and reasonably available steps to

[21] *Id.* at 17.
[22] *Id.* at 28.
[23] *Id.*

prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

Plaintiff Randy Thomas's Experience

111. Prior to the Data Breach, Plaintiff Randy Thomas was employed at Defendant for approximately seventeen years, from 2005 until 2022. In the course of enrolling in employment with Defendant and as a condition of employment, he was required to supply Defendant with his PII, including his name and Social Security number.

112. Mr. Thomas is very careful about sharing his sensitive PII. Mr. Thomas stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

113. At the time of the Data Breach—from November 3, 2022 to November 5, 2022—Defendant retained Mr. Thomas's PII in its system, despite the fact that Mr. Thomas was no longer employed by Defendant.

114. Mr. Thomas received the Notice Letter, by U.S. mail, directly from Defendant, dated February 17, 2023. According to the Notice Letter, Mr. Thomas's PII was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

115. Upon receiving the Notice Letter form Defendant, Mr. Thomas also spent time dealing with the consequences of the Data Breach, including time spent enrolling in credit monitoring and identity theft insurance This time has been lost forever and cannot be recaptured.

116. Subsequent to the Data Breach, Mr. Thomas has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of PII; (ii) invasion of privacy;

(iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

117. Mr. Thomas additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant was the requirement that it adequately safeguard his PII. Mr. Thomas would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

118. Mr. Thomas also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

119. Mr. Thomas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

120. Mr. Thomas has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Gabrielle Thomas's Experience

121. Prior to the Data Breach, Plaintiff Gabrielle Thomas, upon marrying Plaintiff Randy Thomas in or about 2007, received employee-benefits from Defendant as a result of her husband Plaintiff Randy Thomas's employment at Defendant. In the course of enrolling in

employment-benefits with Defendant, she was required to supply Defendant with her PII, including her name and Social Security number.

122. Ms. Thomas is very careful about sharing her sensitive PII. Ms. Thomas stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

123. At the time of the Data Breaches—from November 3, 2022 to November 5, 2022––Defendant retained Ms. Thomas's PII in its system, despite the fact that Ms. Thomas's husband was no longer employed by Defendant.

124. Ms. Thomas received the Notice Letter, by U.S. mail, directly from Defendant, dated February 17, 2023. According to the Notice Letter, Ms. Thomas's PII was improperly accessed and obtained by unauthorized third parties, including her name and Social Security number.

125. Upon receiving the Notice Letter form Defendant, Ms. Thomas also spent time dealing with the consequences of the Data Breach, including time spent enrolling in credit monitoring and identity theft insurance. This time has been lost forever and cannot be recaptured.

126. Subsequent to the Data Breach, Ms. Thomas has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of PII; (ii) invasion of privacy; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

127. Implied in her employment-benefits contract with Defendant was the requirement that it adequately safeguard her PII. Ms. Thomas would not have enrolled in Defendant's benefits plan had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

128. Ms. Thomas also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

129. Ms. Thomas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

130. Ms. Thomas has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Robert MacMichael's Experience

131. Prior to the Data Breach, Plaintiff Robert MacMichael, was employed at Defendant from approximately 2011 until 2012. In the course of enrolling in employment with Defendant and as a condition of employment, he was required to supply Defendant with his PII, including his name and Social Security number.

132. Mr. MacMichael is very careful about sharing his sensitive PII. Mr. MacMichael stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

133. At the time of the Data Breach—from November 3, 2022 to November 5, 2022—Defendant retained Mr. MacMichael's PII in its system, despite the fact that Mr. MacMichael was no longer employed by Defendant.

134. Mr. MacMichael received the Notice Letter, by U.S. mail, directly from Defendant, dated February 17, 2023. According to the Notice Letter, Mr. MacMichael's PII was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

135. Upon receiving the Notice Letter form Defendant, Mr. MacMichael also spent time dealing with the consequences of the Data Breach, including time spent enrolling in credit monitoring and identity theft insurance This time has been lost forever and cannot be recaptured.

136. Subsequent to the Data Breach, Mr. MacMichael has suffered numerous, substantial injuries including, but not limited to: (i) lost or diminished value of PII; (ii) invasion of privacy; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

137. Mr. MacMichael additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant was the requirement that it adequately safeguard his PII. Mr. MacMichael would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

138. Mr. MacMichael also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

139. Mr. MacMichael has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

140. Mr. MacMichael has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class, the Florida Subclass, and the Pennsylvania Subclass)

141. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein

142. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Representative Plaintiffs and Class Members in its computer systems and on its networks.

143. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

b. to protect Representative Plaintiffs' and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected its PII.

144. Defendant knew that the PII was private and confidential and should be protected as private and confidential and thus Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

145. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

146. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PII.

147. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Representative Plaintiffs and Class Members had entrusted to it.

148. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Representative Plaintiffs and Class Members.

149. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

150. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

151. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

152. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Representative Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Representative Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

153. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

154. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

155. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

156. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

157. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

158. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Representative Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

159. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

160. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

161. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

162. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

163. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.*

164. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of its PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to its PII, which may remain in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

165. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

166. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class, the Florida Subclass, and the Pennsylvania Subclass)

167. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

168. This Count is pleaded in the alternative to the unjust enrichment claim below (Third Claim for Relief).

169. Representative Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant or in order to receive employment-related benefits at Defendant.

170. Representative Plaintiffs and Class Members provided their labor and/or PII to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure.

171. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Representative Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

172. Indeed, the Privacy Policy posted on Defendant's website provides that: Indeed, Defendant's Privacy Statement provides that: "[w]e will not sell or rent your information to any third party, and will exercise reasonable efforts to keep the information secure. Cleveland Brothers Equipment Co., Inc. recognizes and respects your online privacy."

173. On information and belief, Defendant further promised to comply with industry standards and to make sure that Representative Plaintiffs' and Class Members' PII would remain protected.

174. Implicit in the agreement between Representative Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Representative Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only

under conditions that kept such information secure and confidential, and (g) delete or destroy PII after it was no longer necessary to retain for employment obligations.

175. When Representative Plaintiffs and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to delete or destroy it following the end of the employment relationship.

176. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

177. In entering into such implied contracts, Representative Plaintiffs and Class Members reasonably believed and expected that Defendant's data security and retention practices complied with relevant laws and regulations and were consistent with industry standards.

178. Representative Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

179. Representative Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

180. Representative Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

181. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

182. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

183. Representative Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

184. Representative Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

185. Representative Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of the Nationwide Class, the Florida Subclass, and the Pennsylvania Subclass)

186. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

187. This Count is pleaded in the alternative to the breach of implied contract claim above (Second Claim for Relief).

188. Representative Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of their labor and/or by providing their valuable PII to Defendant.

189. Representative Plaintiffs and Class Members provided Defendant their labor and/or PII on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. In exchange, Representative Plaintiffs and Class members should have received adequate protection and data security for such PII held by Defendant.

190. Defendant benefited from receiving Representative Plaintiffs' and Class Members' labor and from receiving their PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

191. Defendant knew Representative Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Representative Plaintiffs and Class Members for business purposes.

192. Because all PII provided by Representative Plaintiffs and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it collected from its employees was inherent to the employment relationship.

193. Defendant also understood and appreciated that Representative Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

194. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Representative Plaintiffs and Class Members.

195. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Representative Plaintiffs' and Class Members' PII.

196. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Representative Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Representative Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

197. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Representative Plaintiffs and Class Members, because

Defendant failed to implement appropriate data management and security measures mandated by industry standards.

198. Defendant's enrichment at the expense of Representative Plaintiffs and Class Members is and was unjust.

199. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

200. If Representative Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

201. Representative Plaintiffs and Class Members have no adequate remedy at law.

202. As a direct and proximate result of Defendant's conduct, Representative Plaintiffs and Class Members have suffered and will suffer injury as described herein.

203. Representative Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class, the Florida Subclass, and the Pennsylvania Subclass, respectfully request the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PII of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: June 7, 2023

Respectfully submitted,

/s/ Randi Kassan, Esq.

Randi Kassan, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

David K. Lietz (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Phone: (866) 252-0878
Fax: (202) 686-2877
dlietz@milberg.com

Laura Van Note, Esq. (*Pro Hac Vice* forthcoming)
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Telephone:(510) 891-9800
Facsimile: (510) 891-7030
lvn@colevannote.com

Attorneys for Plaintiffs
and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on June 7, 2023 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Randi Kassan
Randi Kassan